
THE CENTER
FOR INFORMATION
POLICY LEADERSHIP
HUNTON & WILLIAMS LLP

June 12, 2006

Mr. Eric Holloway
U.S. Department of Commerce
1401 Constitution Avenue NW
Room 2806
Washington, DC 20230

Re: Response to a request for comments on the development and implementation of cross-border privacy rules in the Asia Pacific Cooperation Group

Dear Mr. Holloway,

I am pleased to submit these comments on behalf of the Center for Information Policy Leadership at Hunton & Williams LLP in response to the May 22, 2006 Department of Commerce International Trade Administration's request for comments on the development and implementation of cross border privacy rules ("CBPRs") in the Asian Pacific Economic Cooperation ("APEC") region. Founded in 2001, the Center for Information Policy Leadership at Hunton & Williams LLP provides a unique combination of strategic legal and policy thought leadership. Led by internationally recognized privacy and data security professionals, the Center addresses information privacy and security issues from a research-based, non-partisan perspective that seeks to take into account the needs of individuals, the realities of the business environment, and the practical costs and benefits of protecting (or failing to protect) privacy and security. Through its various projects, the Center works with government agencies, businesses, and not-for-profit groups throughout the world to improve the quality and rationality of information policymaking and practice. The Center does not lobby and does not represent clients.

In order to serve the needs of their customers and to stay competitive in a global economy, global businesses must move personally identifiable information to facilities and vendors that are located throughout the APEC region and beyond. This information needs to be protected from inappropriate access, alteration, and harmful misuse as it moves across borders. These data flows are the driving force for economic growth in the APEC region. The APEC Electronic Commerce Steering Group created the APEC Privacy Subgroup to assure these data flows within the APEC region would continue by creating a privacy framework to protect this information. The APEC Privacy Subgroup has established a

THE CENTER
FOR INFORMATION
POLICY LEADERSHIP

HUNTON & WILLIAMS LLP

Mr. Eric Holloway
June 12, 2006
Page 2

framework of nine privacy principles set forth in the APEC Privacy Framework that, when applied, will give governments the confidence to let personally identifiable information about their citizens flow between the twenty-one member APEC economies, each of which have very different legal systems and privacy laws. The APEC Privacy Framework requires that companies that assert that they are APEC compliant be accountable for protecting personally identifiable information consistent with the APEC privacy principles.

The Center believes the APEC Privacy Framework prepared by the APEC Privacy Subgroup and adopted in November 2004 is an excellent document. The APEC Privacy Framework sets forth nine principles that establish a baseline level of protection for personally identifiable information when such information crosses borders. It is now time to put the APEC Privacy Framework into effect. APEC has included international implementation as Part B of the Framework. A key aspect of international implementation involves the support and recognition of CBPRs whereby companies would demonstrate their compliance with the APEC principles and be accountable for their continued compliance. To accomplish that goal and maintain dynamic trade in the APEC region, the following tasks are being completed by APEC through the E-Commerce Steering Group and Privacy Subgroup:

- Developing an instrument that will make it possible for companies to demonstrate that their corporate privacy processes are compliant with the APEC Privacy Framework;
- Establishing procedures by which companies in the APEC region may submit their documentation (the completed instrument with supporting materials) for recognition. Such recognition would then be honored by other APEC economies. This work may be started as a pathfinder by a core group of economies; and
- Establishing enforcement processes to facilitate the transfer of an investigation from an economy where a complaint arises to the economy with jurisdiction over the recognition of a company's CBPR.

The Department's notice asks questions consistent with completing the three tasks mentioned above. The Department's questions are focused on the creation of CBPRs. The Center agrees with that focus, and will respond to groupings of questions.

Mr. Eric Holloway
June 12, 2006
Page 3

Why are CBPRs Needed?

Modern businesses distribute their processes across their entire organization regardless of where operations and facilities are located. Furthermore, businesses are increasingly distributing work to business partners who can do the work in a more efficient and cost effective manner. These new business processes have been facilitated by advances in computer and communication technologies. In virtually all instances, the flow of personally identifiable data across borders is involved and is critical to the business process. The ubiquitous nature of these global transfers runs counter to the cross border data transfer restrictions that are an essential part of the European Data Protection Directive. The European Union prohibits flows of data to economies that do not have adequate privacy protection. The EU has defined adequacy as a system that mirrors the EU system of privacy laws and processes. The EU recognizes other means of permitting the transfer of personally identifiable information such as the EU/US Safe Harbor, model contracts, consent and binding corporate rules. The EU system, however, is not flexible enough to match the speed in which modern markets change. For example, the EU process require companies to anticipate the countries to which transfers will be needed, making it difficult for companies to respond quickly to rapid changes in markets or the need to temporarily relocate personnel. Consequently, the EU system meets neither the consumer's need for economic value nor the protection of personally identifiable information.

The APEC Privacy Framework creates a flexible system for business that facilitates the transfer of personally identifiable information while at the same time provides sufficient protections for that information. It does so by creating a privacy baseline using the nine privacy principles. The ninth privacy principle is accountability. Companies must demonstrate that they are compliant with the principles, and will remain accountable for meeting their obligations under the principles as data moves through the organization and to the organization's business partners. CBPRs are the means by which businesses demonstrate their compliance with the principles. Every economy has its own legal system and privacy culture. The APEC Framework respects the diversity of each economy, and allows data to move in a protected fashion without requiring every economy to adopt the same legal system for privacy.

THE CENTER

FOR INFORMATION
POLICY LEADERSHIP

HUNTON & WILLIAMS LLP

Mr. Eric Holloway

June 12, 2006

Page 4

How do we create CBPRs?

Most companies that are members of the Center for Information Policy Leadership have developed or are in the midst of developing global platforms for privacy. These companies need a means of demonstrating that their privacy processes and procedures match the APEC Privacy Framework. Therefore, the Center believes a detailed questionnaire should be created from the principles. A company would complete the questionnaire and attach supporting materials. The company's global privacy platform is essentially the company's CBPRs, and the completed questionnaire is a means of demonstrating the company's intent to be compliant with the APEC Privacy Framework.

This questionnaire could be developed in one of three ways. First, the Privacy Subgroup could hire a consultant to develop the instrument in cooperation with a working party consisting of Subgroup members. Second, one of the economies could develop a draft questionnaire and submit it to the Subgroup for vetting. Lastly, the questionnaire could be developed by a business advisory group and submitted to the Subgroup for vetting. Regardless of who develops the questionnaire, the Center believes that a questionnaire should be developed this summer in time for discussion at the September Privacy Subgroup meeting.

How CBPRs would be recognized

In order for CBPRs to be effective, they must be recognized by at least a core group of APEC member economies. In order to achieve recognition, CBPRs could be reviewed and recognized either by an official agency of a member economy, or an accountability agent, such as a seal program working under the supervision of a recognized government agency. In either case, the Privacy Subgroup will need to establish guidelines for recognizing a CBPR.

Mechanisms to demonstrate and enforce compliance

In order to be effective, all rules require an enforcement process. APEC principle nine requires a company to be accountable for its compliance with the APEC Privacy Framework. Therefore, a CBPR should include a procedure for receiving and appropriately acting upon inquiries from individuals, accountability agents and economies consistent with the accountability principle. Accountability agents, whether

Mr. Eric Holloway

June 12, 2006

Page 5

they are a seal program or a government agency, should be permitted to review a business's behavior if it appears unresponsive to concerns or there is suspicion that the business has significant violations of its CBPRs. Economies should adopt reasonable penalties for non-compliance.

Mechanisms to foster cooperation among regulatory bodies

In order for CBPRs to be effective, the regulators in the APEC region must cooperate with one another. Currently, the OECD Working Party on Information Security and Privacy has a task group working on means to encourage cooperation among privacy enforcement agencies. The group is exploring impediments to cooperation between the privacy agencies in the APEC member economies and means for building trust among agencies in different countries with different legal systems. Seven countries that are members of OECD are also members of APEC. Rather than duplicating efforts, the Center suggests that APEC work with the OECD Working Party to develop the requisite cooperation between the member economies which is critical for the success of the CBPRs.

Mechanisms to ensure support of the concept of CBPRs by APEC economies

The APEC economies will support processes that foster economic growth in the region. The purpose of the APEC Privacy Framework is to encourage information-facilitated commerce in the region by assuring individuals that their privacy will be protected. The CBPRs, in effect, are the means to implement the APEC Privacy Framework principles. In order to make CBPRs a reality, however, the APEC economies, their citizens and businesses must understand the trade potential associated with alleviating concerns about the inappropriate use and disclosure of information.

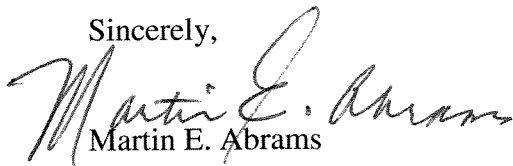
These comments were written by Martin Abrams, Executive Director, Center for Information Policy Leadership, with the assistance of Elisabeth McCarthy, Counsel,

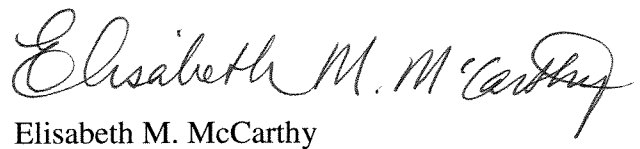
THE CENTER
FOR INFORMATION
POLICY LEADERSHIP
HUNTON & WILLIAMS LLP

Mr. Eric Holloway
June 12, 2006
Page 6

Hunton & Williams LLP. Please submit any questions you have to either Mr. Abrams or Ms. McCarthy. Thank you for the opportunity to submit these comments.

Sincerely,


Martin E. Abrams


Elisabeth M. McCarthy